THE QUADRATIC CHARACTER OF $1+\sqrt{2}$ AND AN ELLIPTIC CURVE

YU TSUMURA

ABSTRACT. When $p \equiv 1 \pmod 8$, we have a criterion of the quadratic character of $1+\sqrt{2}$, which is related to the class number of $\mathbb{Q}(\sqrt{-p})$. In this paper, we obtain a similar criterion using an elliptic curve, which contrasts to the proof using algebraic number theory for the old one.

1. INTRODUCTION.

Let $p \equiv 1 \pmod 8$ be a prime number. Then by the quadratic reciprocity law, 2 is a square mod p, hence there exists $\sqrt{2} \in \mathbb{F}_p$. Also we know that $p \equiv 1 \pmod 8$ can be expressed as $p = c^2 + 8d^2$, where c, d are integers.

In1969, Pierre Barrucand and Harvey Cohn provided the criterion of quadratic character of $1+\sqrt{2}$. Let $\left(\frac{*}{p}\right)$ be the Jacobi symbol mod p. Then they proved the following.

Theorem 1.1. *Let $p = c^2 + 8d^2$ be a prime number, where c, d are integers. Then we have*

$$\left(\frac{1+\sqrt{2}}{p}\right) = 1 \Longleftrightarrow d \equiv 0 \pmod 2 \Longleftrightarrow h(-4p) \equiv 0 \pmod 8,$$

where $h(-4p)$ denotes the class number of $\mathbb{Q}(\sqrt{-p})$.

Proof. See [1] and Proposition 5.15 in [2]. □

This was proved by the method of algebraic number theory. In this article, we provide a slightly different criterion with a different taste proof using properties of an elliptic curve defined by $E : y^2 = x^3 - x$. This proof is simple and more accessible than the old one for those who are familiar with the basics of elliptic curves.

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 11E25.

2. A new criterion

Again let $p \equiv 1 \pmod 8$ be a prime number. Then we can write $p = a^2 + b^2$, where a, b are integers. Further we can assume that a is odd, b is even and $a + b \equiv 1 \pmod 4$. Then we show the following.

Theorem 2.1. *Let notation be as above. Then we have*

$$\left(\frac{1+\sqrt{2}}{p}\right) = 1 \Longleftrightarrow (a-1)^2 + b^2 \equiv 0 \pmod{32}$$

Proof. Let $E(\mathbb{F}_p)$ be an elliptic curve defined by $y^2 = x^3 - x$ over a finite field $\mathbb{F}_p$. We know that $\#E(\mathbb{F}_p) = (a-1)^2 + b^2$. (See Theorem 4.23, page 115 in [3].)

Since $p \equiv 1 \pmod 4$, -1 is a square mod p by the quadratic reciprocity law. So let $i \in \mathbb{F}_p$ be a square root of -1. Then the action of i on a point $(x, y) \in E(\mathbb{F}_p)$ defined by $[i] \cdot (x, y) = (-x, iy)$ is easily seen to be a homomorphism. Actually, $E(\mathbb{F}_p)$ has complex multiplication by $\mathbb{Z}[i]$. (See Example 10.2 in [3].) Let us denote $\eta = 1 + i$. We describe the action of η explicitly. Let $\eta \cdot (x, y) = (x_0, y_0)$. We have

$$\eta \cdot (x, y) = [1 + i] \cdot (x, y) = (x, y) + [i] \cdot (x, y) = (x, y) + (-x, iy).$$

Here i in the y-coordinate is a square root of -1 in $\mathbb{F}_p$. Then by the elliptic curve addition, it is equal to

$$\left(\left(\frac{(1-i)y}{2x}\right)^2, y_0\right) \tag{2.1}$$

$$= \left(\frac{x^2 - m}{2ix}, y_0\right), \tag{2.2}$$

where $y_0 = \left(\frac{(1-i)y}{2x}\right)(x - x_0) - y$. Note that by the equation (2.1), the x-coordinate x_0 of $\eta \cdot (x, y)$ is a square. Also by the equation (2.2), we have $\deg(\eta) = 2$, hence it is easy to see that $\ker(\eta) = \{\infty, (0, 0)\}$, where ∞ denotes the point at infinity (the identity).

Let $x(S)$, $S \subset E(\mathbb{F}_p)$ be the set of x-coordinate of $(x, y) \in S \setminus \{\infty\}$. Now, using (2.2), we see that $x(\eta^{-1}(\infty)) = \{0\}$, $x(\eta^{-2}(\infty)) = \{\pm 1\}$, $x(\eta^{-3}(\infty)) = \{\pm i\}$, $x(\eta^{-4}(\infty)) = \{\pm 1 \pm \sqrt{2}\}$.

Now we prove a claim that $(x_0, y_0) \in E(\mathbb{F}_p)$ has a preimage by η in $E(\mathbb{F}_p)$ if and only if x_0 is a square mod $\mathbb{F}_p$. Suppose x_0 is a square mod p, then we solve equation (2.2). Comparing x-coordinate we have $x_0 = (x^2 - m)/(2ix)$. Solving for x, we have $x = x_0 i + \sqrt{m - x_0^2}$. Since

$\left(\frac{x_0}{p}\right) = 1$, we have

$$\left(\frac{m-x_0^2}{p}\right) = \left(\frac{-y_0^2 x_0^{-1}}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y_0^2}{p}\right)\left(\frac{x_0}{p}\right) = 1.$$

Hence $\sqrt{m-x_0} \in \mathbb{F}_p$ and therefore, we have $x \in \mathbb{F}_p$. Now comparing y-coordinate, we have $y = y_0\left\{\left(\frac{1-i}{2x}\right)(x-x_0)-1\right\}^{-1} \in \mathbb{F}_p$. Then we have $\eta\cdot(x,y) = (x_0,y_0)$ for $(x,y) \in E(\mathbb{F}_p)$.

The converse follows from the equation (2.1).

We finish the consideration of the action of η and now we move to prove the theorem. Suppose $\left(\frac{1+\sqrt{2}}{p}\right) = 1$. Then since

$$\left(\frac{1+\sqrt{2}}{p}\right)\left(\frac{1-\sqrt{2}}{p}\right) = \left(\frac{-1}{p}\right) = 1, \tag{2.3}$$

we have $\left(\frac{1-\sqrt{2}}{p}\right) = 1$. Hence all points whose x-coordinate is one of $\pm 1 \pm \sqrt{2}$ have preimages by η in $E(\mathbb{F}_p)$ by the above claim. Hence $\eta^{-5}(\infty)$ is a subgroup of $E(\mathbb{F}_p)$. Since $\#\eta^{-5}(\infty) = 32$ (note that $\#\ker(\eta) = 2$), we have $32 | \#E(\mathbb{F}_p) = (a-1)^2+b^2$, hence we have $(a-1)^2+b^2 \equiv 0 \pmod{32}$.

Conversely, suppose $(a-1)^2+b^2 \equiv 0 \pmod{32}$. Since $32|\#E(\mathbb{F}_p) = (a-1)^2+b^2$ and $E(\mathbb{F}_p)$ is in general cyclic or a product of two cyclic groups, we have an element $P \in E(\mathbb{F}_p)$ of order 8. Then the x-coordinate of $\eta(P)$ or $\eta^2(P)$ is one of $\pm 1 \pm \sqrt{2}$, say it is Q. Hence Q has a preimage of η. As we saw in the above claim, this means that the x-coordinate of Q is a square mod p. So one of $\pm 1 \pm \sqrt{2}$ is a square. Hence by (2.3), all of them are squares. Especially, we have $\left(\frac{1+\sqrt{2}}{p}\right) = 1$.

□

Comparing these two theorems, we immediately get the following, which seems to difficult to prove elementarily.

Corollary 2.2. *Let $p \equiv 1 \pmod 8$ be a prime number. Let $p = a^2+b^2 = c^2+8d^2$, where a,b,c,d are integers and a is odd, b is even and $a+b \equiv 1 \pmod 4$. Then*

$$(a-1)^2+b^2 \equiv 0 \pmod{32} \Longleftrightarrow d \equiv 0 \pmod 2.$$

References

1. Pierre Barrucand and Harvey Cohn, *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70. MR MR0249396 (40 #2641)

2. Franz Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, From Euler to Eisenstein. MR MR1761696 (2001i:11009)
3. Lawrence C. Washington, *Elliptic curves*, second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008, Number theory and cryptography. MR MR2404461 (2009b:11101)

Department of Mathematics, Purdue University 150 North University Street, West Lafayette, Indiana 47907-2067
E-mail address: ytsumura@math.purdue.edu